

**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings of claims in the application:

**Listing of Claims:**

1                   1. (currently amended) A method performed by a custodian computing system,  
2 having memory, to share a secret  $S$  among  $n$  secret owners, the method comprising the steps of:  
3                   choosing two large primes  $P$  and  $Q$ ;  
4                   computing, at the custodian computing system, a product  $N = PQ$ ;  
5                   computing a product  $M = (P-1)(Q-1)$ ;  
6                   choosing  $n$  random numbers  $q_1$  through  $q_n$  that are relatively prime to  $M$ ;  
7                   determining a number  $d$  such that a product of  $q_1$  through  $q_n$  and  $d \bmod M$  equals  
8 one;  
9                   computing  $S^d$ ;  
10                  distributing  $n$  secret owner pieces to each of the  $n$  secret owners, wherein each of  
11 the secret owner pieces includes  $S^d$  and one of the numbers  $q_1$  through  $q_n$ ; and  
12                  deleting from the custodian computer memory the secret  $S$ ,  $P$ ,  $Q$ ,  $M$ ,  $q_1$  through  
13  $q_n$ , and  $d$ .

1                   2. (original) A method as in claim 1, the method further comprising the steps of:  
2                   receiving a first of the  $n$  secret owner pieces from one of the  $n$  secret owners; and  
3                   computing and storing  $S' = S^{dq} \bmod N$ , where  $q$  represents the one of the numbers  
4  $q_1$  through  $q_n$  contained in the first of the  $n$  secret owner pieces.

1                   3. (original) A method as in claim 2, the method further comprising the steps of:  
2                   receiving a second of the  $n$  secret owner pieces from another one of the  $n$  secret  
3 owners;  
4                   computing  $S^q \bmod N$ , where  $q$  represents the one of the numbers  $q_1$  through  $q_n$   
5 contained in the second of the  $n$  secret owner pieces; and replacing  $S'$  with  $S^q \bmod N$ .

1                   4. (original) A method as in claim 3, further comprising the step of:  
2 each time another of the secret owner pieces is received from another one of the  $n$  secret owners;  
3                   computing  $S'^q \bmod N$ , where  $q$  represents the one of the numbers  $q_1$  through  $q_n$   
4 contained in another of the  $n$  secret owner pieces; and replacing  $S'$  with  $S'^q \bmod N$ .

1                   5. (currently amended) A method performed by a custodian computing system,  
2 having memory, to share a secret  $S$  among  $n$  secret owners, the method comprising the steps of:  
3                   choosing two large primes  $P$  and  $Q$ ;  
4                   computing, at the custodian computing system, a product  $N = PQ$ ;  
5                   computing a product  $M = (P-1)(Q-1)$ ;  
6                   choosing  $n+1$  random numbers  $q_1$  through  $q_n$  and  $d'$  that are relatively prime to  
7  $M$ ;  
8                   determining a number  $d$  such that a product of  $q_1$  through  $q_n$ ,  $d'$ , and  $d \bmod M$   
9 equals one;  
10                  computing  $S^d$ ;  
11                  distributing  $n$  secret owner pieces to each of the  $n$  secret owners, wherein each of  
12 the secret owner pieces includes  $S^d$  and one of the numbers  $q_1$  through  $q_n$ ; and  
13                  deleting from the custodian computer memory the secret  $S$ ,  $P$ ,  $Q$ ,  $M$ ,  $q_1$  through  
14  $q_n$ , and  $d$ .

1                   6. (original) A method as in claim 5, the method further comprising the steps of:  
2 receiving a first of the  $n$  secret owner pieces from one of the  $n$  secret owners; and  
3                   computing and storing  $S' = S^{dq} \bmod N$ , where  $q$  represents the one of the numbers  
4  $q_1$  through  $q_n$  contained in the first of the  $n$  secret owner pieces.

1                   7. (original) A method as in claim 6, the method further comprising the steps of:  
2 receiving a second of the  $n$  secret owner pieces from another one of the  $n$  secret  
3 owners;  
4                   computing  $S'^q \bmod N$ , where  $q$  represents the one of the numbers  $q_1$  through  
5  $q_n$  contained in the second of the  $n$  secret owner pieces; and

6 replacing  $S'$  with  $S'^q \bmod N$ .

1 8. (original) A method as in claim 7, further comprising the step of:  
2 each time another of the secret owner pieces is received from another one of the  $n$   
3 secret owners;

4 computing  $S'^q \bmod N$ , where  $q$  represents the one of the numbers  $q_1$  through  $q_n$

5 contained in the another of the  $n$  secret owner pieces; and

6 replacing  $S'$  with  $S'^q \bmod N$ .

1 9. (original) A method as in claim 8, further comprising the steps of:

2 after all  $n$  secret owner pieces has been received;

3 computing  $S^{d'} \bmod N$ ; and

4 replacing  $S'$  with  $S^{d'} \bmod N$ .

1 10. (currently amended) A method performed by a custodian computing system,  
2 having memory, to share a secret  $S$  among  $n$  secret owners such that any  $k$  of the  $n$  secret owners  
3 may reconstruct the secret, the method comprising the steps of:

4 choosing two large primes  $P$  and  $Q$ , such that  $PQ$  is greater than  $S$ ;

5 computing, at the custodian computing system, and storing in the custodian  
6 computer memory a product  $N = PQ$ ;

7 computing and storing a product  $M = (P-1)(Q-1)$ ;

8 choosing  $n$  random numbers  $e_1$  through  $e_n$  that are relatively prime to  $N$ ;

9 choosing another random number  $e$  that is relatively prime to  $N$ ;

10 choosing  $n$  numbers  $d_1$  through  $d_n$  such that  $e_i d_i \bmod M$  equals one for  $1 \leq i \leq n$ ;

11 choosing another number  $d$  such that  $ed \bmod M$  is equal to one;

12 generating and storing a database of  $\binom{n}{k}$  values, where each value is the product

13 of  $d$  and a unique  $k$  of the  $d_i$  numbers for  $1 \leq i \leq n$ ;

14 deleting from the custodian computer memory  $P$ ,  $Q$ , and  $M$ ;

15 computing  $S^e$ ;

16 distributing  $n$  secret owner pieces to each of the  $n$  secret owners, wherein each of  
17 the secret owner pieces includes  $S^e$  and one of the numbers  $e_1$  through  $e_n$ ; and  
18 deleting the secret  $S$  and  $e_1$  through  $e_n$ ,  $d_1$  through  $d_n$ , and  $d$ .

1 11. (original) A method as in claim 10, the method further comprising the steps  
2 of:  
3 receiving a first of the  $n$  secret owner pieces from one of the  $n$  secret owners; and  
4 computing and storing  $S' = S^{e^f} \bmod N$ , where  $f$  represents the one of the numbers  
5  $e_1$  through  $e_n$  contained in the first of the  $n$  secret owner pieces.

1 12. (original) A method as in claim 11, the method further comprising the steps  
2 of:  
3 receiving a second of the  $n$  secret owner pieces from another one of the  $n$  secret  
4 owners;  
5 computing  $S'^q \bmod N$ , where  $q$  represents the one of the numbers  $e_1$  through  $e_n$   
6 contained in the second of the  $n$  secret owner pieces; and replacing  $S'$  with  $S'^q \bmod N$ .

1 13. (original) A method as in claim 12, further comprising the step of:  
2 each time another of the secret owner pieces is received from another one of the  $n$   
3 secret owners;  
4 computing  $S'^q \bmod N$ , where  $q$  represents the one of the numbers  $e_1$  through  $e_n$   
5 contained in the another of the  $n$  secret owner pieces; and replacing  $S'$  with  $S'^q \bmod N$ .

1 14. (original) A method as in claim 13, further comprising the steps of:  
2 after  $k$  secret owner pieces have been received,  
3 retrieving from the database a value  $c$  from among the  $\binom{n}{k}$  values, wherein the  
4 value  $c$  corresponds to the  $k$  secret owner pieces that were received by the custodian;  
5 computing  $S'^c \bmod N$ ; and  
6 replacing  $S'$  with  $S'^c \bmod N$ .

1                   15. (currently amended) A method performed by a custodian computing system,  
2 having memory, to share a secret  $S$  among  $n$  secret owners such that any  $k$  of the  $n$  secret owners  
3 may reconstruct the secret, the method comprising the steps of:

4                   choosing two large primes  $P$  and  $Q$ , such that  $PQ$  is greater than  $S$ ;  
5                   computing, at the custodian computing system, and storing in the custodian  
6 computer memory a product  $N = PQ$ ;

7                   computing and storing a product  $M = (P-1)(Q-1)$ ;  
8                   choosing  $n$  random numbers  $e_1$  through  $e_n$  that are relatively prime to  $N$ ;  
9                   choosing random numbers  $e$  and  $e'$  that are relatively prime to  $N$ ;  
10                  choosing  $n$  numbers  $d_1$  through  $d_n$  such that  $e_i d_i \bmod M$  equals one for  $1 \leq i \leq n$ ;  
11                  choosing numbers  $d$  and  $d'$  such that  $ed \bmod M$  is equal to one and such that  $e'd'$   
12  $\bmod M$  is equal to one;

13                  generating and storing a database of  $\binom{n}{k}$  values, where each value is the product  
14 of  $d$  and a unique  $k$  of the  $d_i$  numbers for  $1 \leq i \leq n$ ;  
15                  deleting from the custodian computer memory  $P$ ,  $Q$ , and  $M$ ;  
16                  computing  $S^{ee'}$ ;  
17                  distributing  $n$  secret owner pieces to each of the  $n$  secret owners, wherein each of  
18 the secret owner pieces includes  $S^{ee'}$  and one of the numbers  $e_1$  through  $e_n$ ; and  
19                  deleting the secret  $S$  and  $e_1$  through  $e_n$ ,  $e$ ,  $d_1$  through  $d_n$ , and  $d$ .

1                   16. (original) A method as in claim 15, the method further comprising the steps  
2 of:  
3                   receiving a first of the  $n$  secret owner pieces from one of the  $n$  secret owners; and  
4                   computing and storing  $S' = S^{ee'f} \bmod N$ , where  $f$  represents the one of the numbers  
5  $e_1$  through  $e_n$  contained in the first of the  $n$  secret owner pieces.

1                   17. (original) A method as in claim 16, the method further comprising the steps  
2 of:

3 receiving a second of the  $n$  secret owner pieces from another one of the  $n$  secret  
4 owners;

5 computing  $S^q \bmod N$ , where  $q$  represents the one of the numbers  $e_1$  through  $e_n$   
6 contained in the second of the  $n$  secret owner pieces; and replacing  $S'$  with  $S^q \bmod N$ .

1 18. (original) A method as in claim 17, further comprising the step of:  
2 each time another of the secret owner pieces is received from another one of the  $n$   
3 secret owners;

4 computing  $S^q \bmod N$ , where  $q$  represents the one of the numbers  $e_1$  through  $e_n$   
5 contained in the another of the  $n$  secret owner pieces; and replacing  $S'$  with  $S^q \bmod N$ .

1 19. (original) A method as in claim 18, further comprising the steps of:  
2 after  $k$  secret owner pieces have been received,

3 retrieving from the database a value  $c$  from among the  $\binom{n}{k}$  values, wherein the  
4 value  $c$  corresponds to the  $k$  secret owner pieces that were received by the custodian;  
5 computing  $S^c \bmod N$ ;

6 replacing  $S'$  with  $S^c \bmod N$ ;  
7 computing  $S^{d'} \bmod N$ ; and  
8 replacing  $S'$  with  $S^{d'} \bmod N$ .

1 20. (currently amended) A method performed by a custodian computing system,  
2 having memory, to share a secret among  $n$  secret owners such that any  $k$  of the  $n$  secret owners  
3 may reconstruct the secret, the method comprising the steps of:  
4 encrypting the secret so as to generate an encrypted secret;  
5 deleting from the custodian computer memory the secret; and  
6 performing a forward  $k$  out of  $n$  secret sharing algorithm on the encrypted secret  
7 so as to generate  $n$  secret owner pieces.

1 21. (original) A method as in claim 20, further comprising the step of:  
2 distributing the  $n$  secret owner pieces to the  $n$  secret owners.

1           22. (original) A method as in claim 21, further comprising the step of:  
2           receiving  $k$  secret owner pieces from  $k$  secret owners.

1           23. (original) A method as in claim 22, further comprising the step of:  
2           performing a reverse  $k$  out of  $n$  secret sharing algorithm on the  $k$  secret owner  
3 pieces so as to recreate the encrypted secret.

1           24. (original) A method as in claim 23, further comprising the step of:  
2           decrypting the encrypted secret so as to recreate the secret.

1           25. (original) A method as in claim 20, wherein the step of performing a forward  
2  $k$  out of  $n$  secret sharing algorithm includes the steps of:  
3           dividing the encrypted secret into  $k$  pieces; and  
4           performing  $n$  polynomial evaluations at  $n$  points of a degree- $k$  polynomial using  
5 the  $k$  pieces of the encrypted secret as polynomial coefficients;  
6           wherein each of the  $k$  secret owner pieces includes a result of one of the  $n$   
7 polynomial evaluations and a corresponding one of the  $n$  points.

1           26. (original) A method as in claim 25, further comprising the steps of:  
2           distributing the  $n$  secret owner pieces to the  $n$  secret owners;  
3           receiving  $k$  secret owner pieces from  $k$  secret owners; and  
4           performing a reverse  $k$  out of  $n$  secret sharing algorithm on the  $k$  secret owner  
5 pieces so as to recreate the encrypted secret; wherein the step of performing a reverse  $k$  out of  $n$   
6 secret sharing algorithm includes the steps of generating a system of  $k$  linear equations and  
7 solving the system of  $k$  linear equations for the  $k$  pieces of the encrypted secret.

1           27. (original) A method as in claim 26, further comprising the step of:  
2           assembling the  $k$  pieces of the encrypted secret so as to recreate the encrypted  
3 secret; and  
4           decrypting the encrypted secret so as to recreate the secret.

1                   28. (original) A computer readable storage medium having embodied thereon  
2 computer readable program code suitable for programming a computer to perform a method  
3 performed by a custodian to share a secret  $S$  among  $n$  secret owners, the method comprising the  
4 steps of:

5                   choosing two large primes  $P$  and  $Q$ ;  
6                   computing a product  $N = PQ$ ;  
7                   computing a product  $M = (P-1)(Q-1)$ ;  
8                   choosing  $n$  random numbers  $q_1$  through  $q_n$  that are relatively prime to  $M$ ;  
9                   determining a number  $d$  such that a product of  $q_1$  through  $q_n$  and  $d \bmod M$  equals  
10 one;  
11                  computing  $S^d$ ;  
12                  distributing  $n$  secret owner pieces to each of the  $n$  secret owners, wherein each of  
13 the secret owner pieces includes  $S^d$  and one of the numbers  $q_1$  through  $q_n$ ; and  
14                  deleting the secret  $S$ ,  $P$ ,  $Q$ ,  $M$ ,  $q_1$  through  $q_n$ , and  $d$ .

1                   29. (original) A computer readable storage medium having embodied thereon  
2 computer readable program code suitable for programming a computer to perform a method  
3 performed by a custodian to share a secret  $S$  among  $n$  secret owners, the method comprising the  
4 steps of:

5                   choosing two large primes  $P$  and  $Q$ ;  
6                   computing a product  $N = PQ$ ;  
7                   computing a product  $M = (P-1)(Q-1)$ ;  
8                   choosing  $n+1$  random numbers  $q_1$  through  $q_n$  and  $d'$  that are relatively prime to  $M$ ;  
9                   determining a number  $d$  such that a product of  $q_1$  through  $q_n$ ,  $d'$ , and  $d \bmod M$   
10 equals one;  
11                  computing  $S^d$ ;  
12                  distributing  $n$  secret owner pieces to each of the  $n$  secret owners, wherein each of  
13 the secret owner pieces includes  $S^d$  and one of the numbers  $q_1$  through  $q_n$ ; and  
14                  deleting the secret  $S$ ,  $P$ ,  $Q$ ,  $M$ ,  $q_1$  through  $q_n$ , and  $d$ .



1                   30. (original) A computer readable storage medium having embodied thereon  
2 computer readable program code suitable for programming a computer to perform a method  
3 performed by a custodian to share a secret  $S$  among  $n$  secret owners such that any  $k$  of the  $n$   
4 secret owners may reconstruct the secret, the method comprising the steps of:  
5                   choosing two large primes  $P$  and  $Q$ , such that  $PQ$  is greater than  $S$ ;  
6                   computing and storing a product  $N = PQ$ ;  
7                   computing and storing a product  $M = (P-1)(Q-1)$ ;  
8                   choosing  $n$  random numbers  $e_1$  through  $e_n$  that are relatively prime to  $N$ ;  
9                   choosing another random number  $e$  that is relatively prime to  $N$ ;  
10                  choosing  $n$  numbers  $d_1$  through  $d_n$  such that  $e_i d_i \bmod M$  equals one for  $1 \leq i \leq n$ ;  
11                  choosing another number  $d$  such that  $ed \bmod M$  is equal to one;  
12                  generating and storing a database of  $\binom{n}{k}$  values, where each value is the product  
13 of  $d$  and a unique  $k$  of the  $d_i$  numbers for  $1 \leq i \leq n$ ;  
14                  deleting  $P$ ,  $Q$ , and  $M$ ;  
15                  computing  $S^e$ ;  
16                  distributing  $n$  secret owner pieces to each of the  $n$  secret owners, wherein each of  
17 the secret owner pieces includes  $S^e$  and one of the numbers  $e_1$  through  $e_n$ ; and  
18                  deleting the secret  $S$  and  $e_1$  through  $e_n$ ,  $e$ ,  $d_1$  through  $d_n$ , and  $d$ .

1                   31. (original) A computer readable storage medium having embodied thereon  
2 computer readable program code suitable for programming a computer to perform a method  
3 performed by a custodian to share a secret  $S$  among  $n$  secret owners such that any  $k$  of the  $n$   
4 secret owners may reconstruct the secret, the method comprising the steps of:  
5                   choosing two large primes  $P$  and  $Q$ , such that  $PQ$  is greater than  $S$ ;  
6                   computing and storing a product  $N = PQ$ ;  
7                   computing and storing a product  $M = (P-1)(Q-1)$ ;  
8                   choosing  $n$  random numbers  $e_1$  through  $e_n$  that are relatively prime to  $N$ ;  
9                   choosing random numbers  $e$  and  $e'$  that are relatively prime to  $N$ ;

10 choosing  $n$  numbers  $d_1$  through  $d_n$  such that  $e_i d_i \bmod M$  equals one for  $1 \leq i \leq n$ ;  
11 choosing numbers  $d$  and  $d'$  such that  $ed \bmod M$  is equal to one and such that  $e'd'$   
12  $\bmod M$  is equal to one;  
13 generating and storing a database of  $\binom{n}{k}$  values, where each value is the product  
14 of  $d$  and a unique  $k$  of the  $d_i$  numbers for  $1 \leq i \leq n$ ;  
15 deleting  $P$ ,  $Q$ , and  $M$ ;  
16 computing  $S^{ee'}$ ;  
17 distributing  $n$  secret owner pieces to each of the  $n$  secret owners, wherein each of  
18 the secret owner pieces includes  $S^{ee'}$  and one of the numbers  $e_1$  through  $e_n$ ; and  
19 deleting the secret  $S$  and  $e_1$  through  $e_n$ ,  $e$ ,  $d_1$  through  $d_n$ , and  $d$ .

1 32. (original) A computer readable storage medium having embodied thereon  
2 computer readable program code suitable for programming a computer to perform a method  
3 performed by a custodian to share a secret among  $n$  secret owners such that any  $k$  of the  $n$  secret  
4 owners may reconstruct the secret, the method comprising the steps of:  
5 encrypting the secret so as to generate an encrypted secret;  
6 deleting the secret; and  
7 performing a forward  $k$  out of  $n$  secret sharing algorithm on the encrypted secret  
8 so as to generate  $n$  secret owner pieces.

1 33. (original) A computer comprising a processor and a computer readable  
2 storage medium coupled to the processor having embodied thereon processor readable program  
3 code suitable for programming the computer to perform a method performed by a custodian to  
4 share a secret  $S$  among  $n$  secret owners, the method comprising the steps of:  
5 choosing two large primes  $P$  and  $Q$ ;  
6 computing a product  $N = PQ$ ;  
7 computing a product  $M = (P-1)(Q-1)$ ;  
8 choosing  $n$  random numbers  $q_1$  through  $q_n$  that are relatively prime to  $M$ ;

9 determining a number  $d$  such that a product of  $q_1$  through  $q_n$  and  $d \bmod M$  equals  
10 one;  
11 computing  $S^d$ ;  
12 distributing  $n$  secret owner pieces to each of the  $n$  secret owners, wherein each of  
13 the secret owner pieces includes  $S^d$  and one of the numbers  $q_1$  through  $q_n$ ; and  
14 deleting the secret  $S$ ,  $P$ ,  $Q$ ,  $M$ ,  $q_1$  through  $q_n$ , and  $d$ .

1 34. (original) A computer comprising a processor and a computer readable  
2 storage medium coupled to the processor having embodied thereon processor readable program  
3 code suitable for programming a computer to perform a method performed by a custodian to  
4 share a secret  $S$  among  $n$  secret owners, the method comprising the steps of:  
5 choosing two large primes  $P$  and  $Q$ ;  
6 computing a product  $N = PQ$ ;  
7 computing a product  $M = (P-1)(Q-1)$ ;  
8 choosing  $n+1$  random numbers  $q_1$  through  $q_n$  and  $d'$  that are relatively prime to  $M$ ;  
9 determining a number  $d$  such that a product of  $q_1$  through  $q_n$ ,  $d'$ , and  $d \bmod M$   
10 equals one;  
11 computing  $S^d$ ;  
12 distributing  $n$  secret owner pieces to each of the  $n$  secret owners, wherein each of  
13 the secret owner pieces includes  $S^d$  and one of the numbers  $q_1$  through  $q_n$ ; and  
14 deleting the secret  $S$ ,  $P$ ,  $Q$ ,  $M$ ,  $q_1$  through  $q_n$ , and  $d$ .

1 35. (original) A computer comprising a processor and a computer readable  
2 storage medium coupled to the processor having embodied thereon processor readable program  
3 code suitable for programming a computer to perform a method performed by a custodian to  
4 share a secret  $S$  among  $n$  secret owners such that any  $k$  of the  $n$  secret owners may reconstruct the  
5 secret, the method comprising the steps of:  
6 choosing two large primes  $P$  and  $Q$ , such that  $PQ$  is greater than  $S$ ;  
7 computing and storing a product  $N = PQ$ ;  
8 computing and storing a product  $M = (P-1)(Q-1)$ ;

9 choosing  $n$  random numbers  $e_1$  through  $e_n$  that are relatively prime to  $N$ ;  
10 choosing another random number  $e$  that is relatively prime to  $N$ ;  
11 choosing  $n$  numbers  $d_1$  through  $d_n$  such that  $e_i d_i \bmod M$  equals one for  $1 \leq i \leq n$ ;  
12 choosing another number  $d$  such that  $ed \bmod M$  is equal to one;  
13 generating and storing a database of  $\binom{n}{k}$  values, where each value is the product  
14 of  $d$  and a unique  $k$  of the  $d_i$  numbers for  $1 \leq i \leq n$ ;  
15 deleting  $P$ ,  $Q$ , and  $M$ ;  
16 computing  $S^e$ ;  
17 distributing  $n$  secret owner pieces to each of the  $n$  secret owners, wherein each of  
18 the secret owner pieces includes  $S^e$  and one of the numbers  $e_1$  through  $e_n$ ; and  
19 deleting the secret  $S$  and  $e_1$  through  $e_n$ ,  $e$ ,  $d_1$  through  $d_n$ , and  $d$ .

1 36. (original) A computer comprising a processor and a computer readable  
2 storage medium coupled to the processor having embodied thereon processor readable program  
3 code suitable for programming the computer to perform a method performed by a custodian to  
4 share a secret  $S$  among  $n$  secret owners such that any  $k$  of the  $n$  secret owners may reconstruct the  
5 secret, the method comprising the steps of:  
6 choosing two large primes  $P$  and  $Q$ , such that  $PQ$  is greater than  $S$ ;  
7 computing and storing a product  $N = PQ$ ;  
8 computing and storing a product  $M = (P-1)(Q-1)$ ;  
9 choosing  $n$  random numbers  $e_1$  through  $e_n$  that are relatively prime to  $N$ ;  
10 choosing random numbers  $e$  and  $e'$  that are relatively prime to  $N$ ;  
11 choosing  $n$  numbers  $d_1$  through  $d_n$  such that  $e_i d_i \bmod M$  equals one for  $1 \leq i \leq n$ ;  
12 choosing numbers  $d$  and  $d'$  such that  $ed \bmod M$  is equal to one and such that  $e'd'$   
13  $\bmod M$  is equal to one;  
14 generating and storing a database of  $\binom{n}{k}$  values, where each value is the product  
15 of  $d$  and a unique  $k$  of the  $d_i$  numbers for  $1 \leq i \leq n$ ;  
16 deleting  $P$ ,  $Q$ , and  $M$ ;

17                    computing  $S^{ee'}$ ;  
18                    distributing  $n$  secret owner pieces to each of the  $n$  secret owners, wherein each of  
19 the secret owner pieces includes  $S^{ee'}$  and one of the numbers  $e_1$  through  $e_n$ ; and  
20                    deleting the secret  $S$  and  $e_1$  through  $e_n$ ,  $d_1$  through  $d_n$ , and  $d$ .

1                    37. (original) A computer comprising a processor and a computer readable  
2 storage medium coupled to the processor having embodied thereon processor readable program  
3 code suitable for programming the computer to perform a method performed by a custodian to  
4 share a secret among  $n$  secret owner such that any  $k$  of the  $n$  secret owners may reconstruct the  
5 secret, the method comprising the steps of:  
6                    encrypting the secret so as to generate an encrypted secret;  
7                    deleting the secret; and  
8                    performing a forward  $k$  out of  $n$  secret sharing algorithm on the encrypted secret  
9 so as to generate  $n$  secret owner pieces.